AUDITORIA A LA IMPLEMENTACIÓN MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Remitido a:

Gustado Adolfo Araque Ferraro
Presidente

Orlando Bolivar Luna
Gerente Gestión de Riesgos

Ellien Yulieth Rodriguez Rincon
Oficial de Seguridad de la Información

Flor Maria Morales Guerra
Vicepresidente de Soporte Corporativo

Julian Bernardo Salinas Díaz
Director Nacional de Informática y tecnología

Oscar Javier Asprilla Cruz
Asesor de Transformación Digital

Diciembre de 2021

OFICINA ASESORA DE CONTROL INTERNO

Tabla de contenido

I. Objetivos 3
II. Metodología utilizada 3
III. Alcance 3
IV. Resultados de la Auditoría 3
V. Conclusiones 14

I. Objetivos

- Realizar auditoría Interna al Sistema de Gestión de Seguridad de la Información y Ciberseguridad.

- Realizar un análisis del estado actual del Sistema de Gestión de Seguridad de la Información bajo los parámetros establecidos en el Modelo de Seguridad y Privacidad de la Información establecido por el MINTIC.

II. Metodología utilizada

- φ Revisión Documental
- φ Confirmación de Información

III. Alcance

Sistema de Gestión de Seguridad de la Información y Ciberseguridad Implementado en la Entidad.

IV. Resultados de la Auditoría

En el mes de febrero de 2020 la Entidad realizó el diagnóstico del MSPI implementado en ese momento, obteniendo como resultado 31% de madurez, razón por la cual a través del Oficial de Seguridad de la Información y Ciberseguridad se inicia el plan de implementación del MSPI – establecido por el MINTIC.

El Plan de Seguridad y Privacidad de la Información el cual hace parte del plan estratégico de la entidad y se encuentra cargado en Cronos, tiene como fecha de inicio el 01 de enero de 2021 y fecha de finalización el 31 de diciembre de 2021, con un total de 37 actividades.

Observación No 01: Incumplimiento del cronograma establecido para la Implementación del Modelo de Seguridad y Privacidad de la Información establecido por MINTIC.

Al revisar el avance de ejecución de las actividades contempladas en el sistema Cronos para la implementación del MSPI se encontró que esté va en un 76% de ejecución teniendo incumplida la siguiente actividad:

1. Elaborar documentación para la operación y gestión del SOC – CSIRT (Centro de Operaciones de Ciberseguridad) a través de servicios tercerizados.

Evidencias de la Observación:

a) Cronograma establecido en Cronos

b) Comunicado SIC-I-042 de Seguridad de la Información

Acción Preventiva Sugerida: Generar todas las actividades necesarias para dar cumplimiento a la actividad en el menor tiempo posible.

A. Fase de Diagnóstico

En esta fase se contempla el resultado del diligenciamiento de la herramienta de diagnóstico establecida por MINTIC – así como la primera evolución de madurez del sistema el cual para el mes de febrero de 2020 se encontraba en un 31%.

Hallazgo No 01: Las pruebas de vulnerabilidad realizadas en la fase de diagnóstico no contemplaron los 28 sistemas de la Entidad tal como lo establece la Guía No 01 del MSPI.

Se evidencio solo dos informes de pruebas de vulnerabilidad realizados al sistema Sherlock y al sistema de los biométricos dos de las 28 aplicaciones que tiene la entidad instalada, la Guía es muy clara en indicar que estas pruebas se deben realizar a todos los sistemas para poder establecer el grado de madurez inicial del Sistema de Gestión de Seguridad y Privacidad de la Información

Evidencias del hallazgo:

a) Guía No 01 Metodología Pruebas de efectividad
b) 06. INF_AnalisisVulnerabilidades_4-72_Sherlock (1)
c) 07. INF_EH_2021_472_SPN-EH_Biometrico_v2
d) LISTADO APLICACIONES – LICENCIAS
e) Comunicado No SIC-I-042 de Seguridad de la Información

Acción Correctiva Sugerida: Generar un cronograma que permita realizar un ciclo que garantice las pruebas de vulnerabilidad a la totalidad de las aplicaciones de la entidad priorizando las de mayor impacto.

B. Fase de Planeación

En este numeral se evaluaron las guías de implementación establecidas en el MSPI – MINTIC, con la respectiva documentación tanto la solicitada por esta Oficina Asesora de Control Interno a través del CIEC 225-e 2021 del 17 de noviembre de 2021 y el 13 de diciembre de 2021, como los documentos que se encuentran en el sistema ISOLUCIÓN

1. Políticas y Procedimientos:

Al Evaluar la documentación del Sistema de Gestión de Seguridad de la Información, con lo indicado en el Modelo de Seguridad y Privacidad de la Información se encontró:

Observación No 02: La Entidad no cuenta con una Política de Disponibilidad del servicio e información como lo establece la Guía No 02 del MSPI – MINTIC:

Teniendo en cuenta que, la administración de la red de comunicaciones y el data center de la Entidad se encuentra tercerizado, para esta Oficina Asesora de Control Interno, es importante que se cuente con una política de disponibilidad del servicios e información establecida y que esta sea de obligatorio cumplimiento para el contratista, con el objetivo de garantizar el efectivo cumplimiento de los servicios de información sin afectar el cumplimiento de la Misión Institucional de la Entidad.

Evidencias de la Observación:

a) Guía No 02 del MSPI
b) Manual de Políticas de Seguridad de la Información y Ciberseguridad – MN-GS-SI-007
c) Comunicado No SIC-I-042 de Seguridad de la Información

Acción Preventiva Sugerida: Generar una política de Disponibilidad de Servicios e Información que sea de obligatoriedad cumplimiento tanto para la Entidad como para los terceros que realicen a la administración de la red y el Data Center.

Hallazgo No 02: No se encontraron los procedimientos de: capacitación y sensibilización del personal, controles criptográficos, gestión de llaves criptográficas, gestión de capacidad, protección contra códigos maliciosos y transferencia de información, establecidos en la Guía No 03 del MSPI - MINTIC

Al revisar los siguientes procedimientos y compararlos con la Guía No 03 del MSPI se encontró que de los 22 procedimientos que requiere la guía solo 6 (27% de los procedimientos) no se encontraron documentados:

Procedimientos indicados en la Guía No 3	Procedimiento	Observación
PROCEDIMIENTO DE CAPACITACIÓN Y SENSIBILIZACIÓN DEL PERSONAL	PR-GH-007	La entidad cuenta con un procedimiento de capacitaciones, sin embargo, en Seguridad de la Información solo se da en la Inducción, en el manual de políticas se establece el tema de capacitaciones y sensibilizaciones, sin embargo, en el procedimiento establecido por gestión humana no se contempla una programación de manera periódica capacitaciones sobre SI, como lo contempla la guía No 03 del MSPI
PROCEDIMIENTO DE CONTROLES CRIPTOGRÁFICOS	No hay Procedimiento	La entidad cuenta una política de criptografía, pero no hay un procedimiento como lo contempla la guía No 03 del MSPI
PROCEDIMIENTO DE GESTIÓN DE LLAVES CRIPTOGRÁFICAS	MN-GI-IT-001/Numeral 5.8.3	El procedimiento establece la gestión de contraseñas de alto perfil, sin embargo, no habla de llaves criptográficas como lo contempla la guía No 03 del MSPI
PROCEDIMIENTO DE GESTION DE CAPACIDAD	No hay Procedimiento	En el documento de Manual de políticas de Tecnología - MN-GI-IT-001 dentro del documento menciona la gestión de capacidad de los sistemas de información, sin embargo, no hay procedimiento establecido como lo contempla la guía No 03 del MSPI
PROCEDIMIENTO DE PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS	No hay Procedimiento	En el documento de Manual de políticas de Tecnología - MN-GI-IT-001 dentro del documento menciona el manejo de virus

Procedimientos indicados en la Guía No 3	Procedimiento	Observación
		y el antivirus, sin embargo, no hay procedimiento establecido como lo contempla la guía No 03 del MSPI
PROCEDIMIENTO DE TRANSFERENCIA DE INFORMACIÓN	No hay Procedimiento	La entidad cuenta una política de transferencia de información, pero no hay un procedimiento como lo contempla la guía No 03 del MSPI

Fuente: Elaboración Propia

Evidencias del Hallazgo

a) Manual de Políticas de Tecnología MN-IT-GI-IT-001
b) Guía No 03 del MSPI – MINTC
c) Correo Electrónico de la DNIT del 28 de diciembre de 2021

Acción Correctiva Sugerida: Generar las actividades necesarias para la creación y modificación de los procedimientos de la Entidad con el objetivo de dar cumplimiento a la Guía No 03 del MSPI - MINTC

2. Tratamiento de Riesgos de Seguridad y Ciberseguridad de la Información.

El Plan de tratamiento de Riesgos de Seguridad y Privacidad establecido por el proceso de Seguridad de la Información, tiene fecha de inicio el 01 de enero de 2021 y fecha de finalización del 15 de enero de 2022, el cual registra un avance del 77%,

Hallazgo No 03: Los Procesos de Marketing, Transformación Digital y Proyectos de Inversión, así como la totalidad de los procesos y subprocesos a nivel regional no cuenta de manera particular con la matriz de riesgos de seguridad y ciberseguridad de la información, tal como lo establece el alcance del Manual de Políticas de Seguridad de la Información y Ciberseguridad – MN-GS-SI-007 Vigente a 30 de diciembre de 2021:

Los Procesos de Marketing, Transformación Digital y Proyectos de Inversión, así como la totalidad de los procesos y subprocesos a nivel regional no cuentan de manera particular con la matriz de riesgos de seguridad y ciberseguridad de la información incumpliendo con el alcance del Manual de Políticas de seguridad y Ciberseguridad de la Información de la Entidad y dado que los riesgos a tratar en el SGSI son los relacionados con los activos de información los cuales son de vital importancia en el MSPI, es necesario que se cubra el 100% de los procesos y subprocesos con los cuenta la entidad tanto a nivel regional – local puesto que las condiciones pueden varias según su ubicación.

Evidencias del hallazgo:

a) Matrices de Riesgo Seguridad de la Información y Ciberseguridad

Acción Correctiva Sugerida: Realizar todas las actuaciones necesarias para completar la identificación, clasificación, generar controles y planes de acción para los procesos faltantes.

Observación No 03: Matrices de Riegos en los cuales no es claro a que subproceso pertenecen:

A través del método aleatorio simple con un con un margen de error del 5% y un nivel de confianza de la muestra del 95% fueron seleccionados aleatoriamente 10 (30% de las matrices entregadas) matrices de riegos para evaluar el cumplimento de estas con lo establecido en la Guía No 07 del MSPI, encontrando que para los siguientes procesos es confuso a que proceso o subproceso se le está realizando la identificación de los riesgos:

Proceso según formato	Análisis del Riesgo					Eva. Riesgo	Val. controles		Observaciones
	I - Rie	I - Act	I - Ame	I - Con	I - Vul	I - Con	Val. Riesgo	Plan Acción	
SST / Selección y Vinculación / Capacitación y Bienestar / Nómina / Retiro	x	x	x	x	x	x	x	x	El nombre del archivo dice que el subproceso es SST sin embargo en el formato menciona más subprocesos
SST / Selección y Vinculación / Capacitación y Bienestar / Nómina / Retiro	x	x	x	x	x	x	x	x	El nombre del archivo dice que el subproceso es Nomina sin embargo en el formato menciona más subprocesos
SST / Selección y Vinculación / Capacitación y Bienestar / Nómina / Retiro	x	x	x	x	x	x	x	x	El nombre del archivo dice que el subproceso es de Bienestar y Capacitaciones sin embargo en el formato menciona más subprocesos
FILATELIA - VENTAS - CANAL RETAIL (PUNTO DE VENTA - ALIADOS Y EXPENDIOS)	x	x	x	x	x	x	x	x	El nombre del archivo dice que el subproceso es de puntos de venta sin embargo en el formato menciona más subprocesos
FILATELIA - VENTAS - CANAL RETAIL (PUNTO DE VENTA - ALIADOS Y EXPENDIOS)	x	x	x	x	x	x	x	x	El nombre del archivo dice que el subproceso es de Filatelia sin embargo en el formato menciona más subprocesos
FILATELIA - VENTAS - CANAL RETAIL (PUNTO DE VENTA - ALIADOS Y EXPENDIOS)	x	x	x	x	x	x	x	x	El nombre del archivo dice que el subproceso es de Ventas sin embargo en el formato menciona más subprocesos

Fuente: Elaboración Propia

Evidencias de la Observación

a) Matrices de Riesgo de la Seguridad de la información.

Acción Preventiva Sugerida: Revisar las matrices de riesgo y ajustarlas el nombre del proceso y subproceso a aquel que se esta evaluando de manera independiente y que este coincida con el nombre del archivo.

3. Controles Establecidos en la Guía No 08 del MSPI

En el mes de octubre de 2021 esta Oficina Asesora de Control Interno realizó el Diagnóstico del estado del Sistema Integrado de Gestión – SIG en la que se incluyó el estado de implementación del Sistema de Gestión de Seguridad y Privacidad de la Información – ISO 27001:2013 y la Guía No 08 del MSPI contempla lo 114 controles que hacen parte del Anexo A de la norma, se comparó la Declaración de Aplicabilidad donde se estableció para la entidad la implementación de 113 Controles de los 114 que contempla la norma.

Al revisar en el Sistema ISOLUCION los hallazgos del diagnóstico y la preauditoria realizada por ICONTEC el primero de diciembre del presente año, se encontró que de los 113 controles que se deberían implementar 37 (33% de los controles) de ellos presentan hallazgo:

Núm.	Nombre	Selección / Excepción	Descripción / Justificación	Hallazgos en ISOLUCION	Tienen Plan de Acción
A.6.1.5	Seguridad de la información en la gestión de proyectos	S	Control: La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto.	Tiene Hallazgo	Si
A.8.1.3	Uso aceptable de los activos	S	Control: Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	Tiene Hallazgo	No
A.8.2.3	Manejo de activos	S	Control: Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Tiene Hallazgo	No
A.9.1.1	Política de control de acceso	S	Control: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	Tiene Hallazgo	No
A.9.2.1	Registro y cancelación del registro de usuarios	S	Control: Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	Tiene Hallazgo	No
A.9.2.3	Gestión de derechos de acceso privilegiado	S	Control: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.	Tiene Hallazgo	No
A.9.2.5	Revisión de los derechos de acceso de usuarios	S	Control: Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.	Tiene Hallazgo	Si

Núm.	Nombre	Selección / Excepción	Descripción / Justificación	Hallazgos en ISOLUCION	Tienen Plan de Acción
A.9.2.6	Retiro o ajuste de los derechos de acceso	S	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.	Tiene Hallazgo	No
A.10.1.1	Política sobre el uso de controles criptográficos	S	Control: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	Tiene Hallazgo	Si
A.11.1.1	Perímetro de seguridad física	S	Control: Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información.	Tiene Hallazgo	Si
A.11.1.2	Controles físicos de entrada	S	Control: Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.	Tiene Hallazgo	Si
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	S	Control: Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	Tiene Hallazgo	Si
A.11.1.4	Protección contra amenazas externas y ambientales	S	Control: Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	Tiene Hallazgo	Si
A.11.1.5	Trabajo en áreas seguras	S	Control: Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.	Tiene Hallazgo	Si
A.11.2.1	Ubicación y protección de los equipos	S	Control: Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.	Tiene Hallazgo	No
A.11.2.2	Servicios de suministro	S	Control: Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Tiene Hallazgo	No
A.11.2.3	Seguridad del cableado	S	Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño.	Tiene Hallazgo	No
A.11.2.4	Mantenimiento de equipos	S	Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.	Tiene Hallazgo	No
A.11.2.9	Política de escritorio limpio y pantalla limpia	S	Control: Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las	Tiene Hallazgo	No

Núm.	Nombre	Selección / Excepción	Descripción / Justificación	Hallazgos en ISOLUCION	Tienen Plan de Acción
			instalaciones de procesamiento de información.		
A.12.1.1	Procedimientos de operación documentados	S	Control: Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.	Tiene Hallazgo	No
A.12.1.3	Gestión de capacidad	S	Control: Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.	Tiene Hallazgo	No
A.12.2.1	Controles contra códigos maliciosos	S	Control: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos. A.12.3 Copias de respaldo Objetivo: Proteger contra la perdida de datos.	Tiene Hallazgo	Si
A.12.3.1	Respaldo de información	S	Control: Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada. A.12.4 Registro y seguimiento Objetivo: Registrar eventos y generar evidencia.	Tiene Hallazgo	Si
A.12.4.2	Protección de la información de registro	S	Control: Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.	Tiene Hallazgo	Si
A.12.6.1	Gestión de las vulnerabilidades técnicas	S	Control: Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	Tiene Hallazgo	No
A.13.1.1	Controles de redes	S	Control: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.	Tiene Hallazgo	No
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	S	Control: Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	Tiene Hallazgo	No
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	S	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	Tiene Hallazgo	No
A.14.2.2	Procedimientos de control de	S	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían	Tiene Hallazgo	Si

Núm.	Nombre	Selección / Excepción	Descripción / Justificación	Hallazgos en ISOLUCION	Tienen Plan de Acción
	cambios en sistemas		controlar mediante el uso de procedimientos formales de control de cambios.		
A.14.2.5	Principios de construcción de sistemas seguros	S	Control: Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	Tiene Hallazgo	Si
A.14.2.6	Ambiente de desarrollo seguro	S	Control: Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	Tiene Hallazgo	Si
A.14.2.7	Desarrollo contratado externamente	S	Control: La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	Tiene Hallazgo	Si
A.14.2.8	Pruebas de seguridad de sistemas	S	Control: Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad.	Tiene Hallazgo	Si
A.14.2.9	Prueba de aceptación de sistemas	S	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.	Tiene Hallazgo	Si
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	S	Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	Tiene Hallazgo	No
A.17.1.2	Implementación de la continuidad de la seguridad de la información	S	Control: La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	Tiene Hallazgo	Si
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	S	Control: La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	Tiene Hallazgo	Si

Fuente: Elaboración Propia

Hallazgo No 04: Hallazgos sin tratamiento a en la Herramienta ISOLUCION a 20 de diciembre de 2021 incumpliendo el Procedimiento Auditorías Internas de Sistemas de Gestión - PR-EC-004 en su numeral 5 actividad 11

Al revisar en la Herramienta ISOLUCION el estado de los planes de acción para cado uno de los 37 hallazgos encontrados en el diagnostico de Control Interno y la preauditoria de ICONTEC, **18 de ellos a corte de 20 de diciembre de 2021 se encontraron sin plan de acción:**

Núm.	Nombre	Selección / Excepción	Descripción / Justificación	Hallazgos en ISOLUCION	Tienen Plan de Acción
A.8.1.3	Uso aceptable de los activos	S	Control: Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	Tiene Hallazgo	No
A.8.2.3	Manejo de activos	S	Control: Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Tiene Hallazgo	No
A.9.1.1	Política de control de acceso	S	Control: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	Tiene Hallazgo	No
A.9.2.1	Registro y cancelación del registro de usuarios	S	Control: Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	Tiene Hallazgo	No
A.9.2.3	Gestión de derechos de acceso privilegiado	S	Control: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.	Tiene Hallazgo	No
A.9.2.6	Retiro o ajuste de los derechos de acceso	S	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.	Tiene Hallazgo	No
A.11.2.1	Ubicación y protección de los equipos	S	Control: Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.	Tiene Hallazgo	No
A.11.2.2	Servicios de suministro	S	Control: Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Tiene Hallazgo	No
A.11.2.3	Seguridad del cableado	S	Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño.	Tiene Hallazgo	No

Núm.	Nombre	Selección / Excepción	Descripción / Justificación	Hallazgos en ISOLUCION	Tienen Plan de Acción
A.11.2.4	Mantenimiento de equipos	S	Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.	Tiene Hallazgo	No
A.11.2.9	Política de escritorio limpio y pantalla limpia	S	Control: Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	Tiene Hallazgo	No
A.12.1.1	Procedimientos de operación documentados	S	Control: Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.	Tiene Hallazgo	No
A.12.1.3	Gestión de capacidad	S	Control: Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.	Tiene Hallazgo	No
A.12.6.1	Gestión de las vulnerabilidades técnicas	S	Control: Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	Tiene Hallazgo	No
A.13.1.1	Controles de redes	S	Control: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.	Tiene Hallazgo	No
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	S	Control: Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	Tiene Hallazgo	No
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	S	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	Tiene Hallazgo	No
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	S	Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	Tiene Hallazgo	No

Fuente: Elaboración Propia

Evidencias del Hallazgo

a) Reporte de Mejora de ISOLUCION http://172.18.165.114/IsolucionCalidad/Mejoramiento/frmFiltroAccion.aspx?TipoAccion=Mg%3d%3d fecha de consulta 20/12/2021

Acción Correctiva Sugerida: Realizar todas las gestiones pertinentes para el tratamiento efectivo de los hallazgos que se encuentran cargados en ISOLUCION.

C FASE DE IMPLEMENTACIÓN

Por último, se evaluaron los indicadores de gestión cargados en ISOLUCIÓN para le proceso de Seguridad de la Información y Ciberseguridad:

Observación No 04: El proceso de Seguridad de la Información y Ciberseguridad no tiene registros de medición para el indicador "Cumplimiento de los requisitos de seguridad de la información y ciberseguridad en los colaboradores y proveedores" en el sistema ISOLUCION.

El Sistema de Gestión de Seguridad de la Información cuenta con dos indicadores que permiten generar una medición de la madurez de este, en la herramienta Thanos, sin embargo, en la Herramienta de ISOLUCION se cuenta también dos indicadores los cuales solo para el indicador "Cumplimiento de los requisitos de seguridad de la información y ciberseguridad en los colaboradores y proveedores" no se cuentan con datos.

Evidencias de la Observación:

a) Indicadores reportados en ISOLUCION http://172.18.165.114/IsolucionCalidad/Medicion/frmReportesBase.aspx?TipoAccion=Mg%3d%3d&Medicion=MQ%3d%3d fecha de consulta 20/12/2021

Acción Preventiva Sugerida: Realizar las actividades necesarias para iniciar con la medición al indicador de "Cumplimiento de los requisitos de seguridad de la información y ciberseguridad en los colaboradores y proveedores".

V. Conclusiones

- ✓ Al realizar la evaluación del estado de la implementación del Modelo de Seguridad y Privacidad de la Información se encuentra en un 76%, con la actividad Elaborar documentación para la operación y gestión del SOC – CSIRT (Centro de Operaciones de Ciberseguridad) a través de servicios tercerizados sin cumplirse generando así observación No 01

- ✓ La entidad viene trabajando en la implementación del MSPI, es importante fortalecer la totalidad de políticas y procedimientos que contempla el modelo establecido por MINTIC – generando las observaciones No 02 y 3 y los hallazgos del 1 al 4.

- ✓ El sistema cuenta con indicadores que permiten medir su nivel de madurez y facilidad en la toma de decisiones, por tal razón es importante que el indicador “Cumplimiento de los requisitos de seguridad de la información y ciberseguridad en los colaboradores y proveedores cuente con datos para su análisis lo que generó la observación No 04.

Cordialmente,

Firmado por:
Josefina Del Pilar Rodriguez Arias
2021/12/30 02:58:29:551

JOSEFINA DEL PILAR RODRIGUEZ ARIAS
Jefe Oficina Asesora de Control Interno

Elaborado por: Yeimy Pérez Sanmiguel – Profesional de Control Interno / Rol Auditor de Sistemas
TDR: 130.02.01 – Auditorías Internas – Auditoria al MSPI 2021